OPENING STATEMENT OF SENATOR BURNS
HEARING ON INTERNET SECURITY
SENATE COMMUNICATIONS SUBCOMMITTEE
MARCH 8, 2000

I would like to welcome everyone to today's hearing, which is the first in a series of hearings this Subcommittee will be holding on the critical issues of Internet security and privacy facing our nation. Today's hearing will focus on the unprecedented and apparently coordinated recent series of hacker attacks which caused some of the most popular websites on the Internet to go dark. The list of sites that were brought down included such Internet mainstays as Amazon.com, eBay, cnn.com, e-Trade and Yahoo.

These attacks are technically called "distributed denial of service attacks" which in plain English is like a telephone system getting overwhelmed by more calls than it can handle. It appears the hackers planned their attacks months in advance, going so far as to set up software on many servers all over the Internet that was capable of automatically flooding targeted websites at certain predetermined times. I suppose it's no surprise that these malicious programs are called "daemons." The hackers involved in theses attacks have yet to be caught, despite the coordinated efforts of our nation's top law enforcement agencies.

While no consumer data was stolen, real damage was done-especially to Internet users' confidence about the security of the systems they are using. The fear of future attacks was great enough to cause a massive selloff in technology stocks in early February when the attacks took place. The nature of these attacks is particularly alarming, as they were specifically designed to disrupt electronic commerce.

The growth of electronic commerce and the Internet in general has been astounding. The number of small businesses on the Web is doubling every year, and currently over 2 million small businesses in the United States have websites. In my home state of Montana, companies such as Vanns.com and Streaming Solutions are showing that all it takes is a great idea and hard work to reach global markets through the Internet. The e-commerce potential of the Internet still has tremendous upside--while household spending online doubled last year, it still amounted to less than 1% of total retail dollars.

The growth and reach of the Internet is a double-edged sword, however. Unfortunately, we now live in a world where malicious criminals can bring large parts of the nation's critical information infrastructure to a grinding halt.

Given the seriousness of these attacks, we must act quickly and effectively. We need to do everything possible to foster better coordination between government and industry in protecting Internet security, make sure our national security and law enforcement agencies have the resources to do their jobs and bring our nation's criminal code up-to-date with the recent development of the Internet.

Clearly, the current level of coordination between government agencies and the private sector needs to

be as seamless and effective as possibe. A core component in achieving this cooperation is the continuing development of the FBI's National Infrastructure Protection Center, which was setup two years ago to deal with a range of potential attacks on the Internet. I strongly supported the creation of the Center and continue to support its full funding.

However, I am concerned that while the Center is authorized for 133 employees, its staff is still at only 100, 40 of whom are detailees from other agencies. I also understand the FBI is still short of its goal of hiring 250 field agents
to fight cybercrime. While I realize that hiring top-level technical experts to work in the government is difficult given the lure of Silicon Valley, these positions need to be filled as quickly as possible.

I want to touch on the issue of criminal penalties on hackers. In the recent past, many if not most "hacker" attacks were the product of intellectual curiosity rather than malicious intent to cause damage. Now, however, the vast majority of hacker attacks are done through simply downloading pre-existing programs from hacker sites on the web and using them to accomplish destructive aims. Rather than stemming from misdirected teenage rebellion, current attacks are often engaged in by adults who want to inflict the most damage possible. We need to severely punish these criminals-and they are criminals. The destruction of data belonging to innocent individuals is no less a crime than property destruction of the more traditional type. In fact, it can in many cases be far worse.

We are fortunate to have some of the foremost government and industry experts in the field of Internet security with us today. I look forward to the testimony of the witnesses in addressing these matters of critical importance to the continued development of e-commerce and the Internet. Thank you.